Detection of Denial-of-Service Attacks Based on Computer Vision Techniques

A Thesis Submitted for the Degree of
Doctor of Philosophy

By

Zhiyuan Tan

in

Faculty of Engineering and Information Technology
UNIVERSITY OF TECHNOLOGY, SYDNEY
AUSTRALIA
19TH DECEMBER 2013

CERTIFICATE

Date: **19th December 2013**

Author: **Zhiyuan Tan**

Title: **Detection of Denial-of-Service Attacks Based on Computer Vision Techniques**

Degree: **Ph.D.**

I certify that this thesis has not already been submitted for any degree and is not being submitted as part of candidature for any other degree.

I also certify that the thesis has been written by me and that any help that I have received in preparing this thesis, and all sources used, have been acknowledged in this thesis.

Signature of Author

Acknowledgements

I am greatly indebted to my supervisor, Xiangjian He for his continuous encourgement, advice, help and invaluable suggestions. He is such a nice, generous, helpful and kindhearted person. I feel really happy, comfortable and unconstrained with him during my PhD study. I owe my research achievements to his experienced supervision. Many thanks are also due to my co-supervisors, Priyadarsi Nanda and Ren Ping Liu for their valued suggestions and constant support, and for the numerous conversations with them. I gratefully acknowledge the useful discussions with Aruna Jamdagni and Qiang Wu. I appreciate the travel support for attending the international conferences which I received from the Faculty of Engineering and IT and the Vice-Chancellor's Conference Fund. I wish to thank my fellow research students and the staff of the school, especially those people listed below for providing various assistance for the completion of this research work.

- Wenjing Jia, Min Xu, Yida Xu, Massimo Piccardi, Doan B. Hoang, Mao Lin Huang, Valerie Gay, Jinjun Chen, Karla Felix Navarro, Ruo Du, Cao Zeng, Sheng Wang, Muhammad Abul Hasan, Man To Wang, Mohammed Ambu Saidi, Ava Bargi, Thawatchai Chomsiri, Mian Ahmad Jan, Yi Wan and Minqi Li.

I would like to thank my wife, Shanshan, for her understanding and assistance. I also thank my parents for the freedom to study for the long time necessary to complete postgraduate studies. This thesis could not have been completed without the support and encouragement of my mother-in-law. My special thanks go to my best friends, Ming Deng and Susan Lai for their continuous care and wishes.

Last but not least, the financial assistance of a University of Technology Sydney International Research Scholarship and a CSIRO ICT Centre Top-up Scholarship is gratefully appreciated.

To My Family

Table of Contents

List of Tables

List of Figures

Abbreviation

Abbreviations	**Descriptions**
ABC	Association Based Classification
ANN	Artificial Neural Networks
AR	Auto-regression
BF	Basic Feasible
bPDM	bivariate Parametric Detection Mechanism
CAT	Change Aggregation Trees
CIDS	Collaborative Intrusion Detection System
CPM	Change-Point Monitoring
CUSUM	Cumulative Sum
DEMD	Differential Earth Mover's Distance
DoS	Denial-of-Service
DDoS	Distributed Denial-of-Service
DR	Detection Rate
EDM	Euclidean Distance Map
EMD	Earth Mover's Distance
EMD-L_1	EMD with L_1 distance
FPR	False Positive Rate
FNR	False Negative Rate
FN	False Negative
FP	False Positive
GDI	Global Defence Infrastructure

Abbreviations	**Descriptions**
GSAD	Geometrical Structure Anomaly Model
ISP	Internet Service Provider
LDA	Linear Discriminant Analysis
LDSes	Local Detection Systems
LP	Linear Programming
MARS	Multivariate Adaptive Regression Splines
MCA	Multivariate Correlation Analysis
MD	Mahalanobis Distance
MDM	Mahalanobis Distance Map
MIB	Management Information Based
PCA	Principal Component Analysis
PoD	Ping of Death
RBFNN	Radial Basis Function Neural Networks
RePIDS	Real-time Payload-based IDS
ROC	Receiver Operating Characteristic
TAM	Triangle Area Map
TCB	Transmission Control Block
TCP	Transmission Control Protocol
TNR	True Negative Rate
TN	True Negative
TP	True Positive
SIP	Secure Infrastructure Protocol
SNMP	Simple Network Management Protocol
SPRT	Sequential Probability Ratio Test
SVM	Support Vector Machine
UDP	User Diagram Protocol
ICMP	Inter Control Message Protocol

Abstract

A Denial-of-Service (DoS) attack is an intrusive attempt, which aims to force a designated resource (e.g., network bandwidth, processor time or memory) to be unavailable to its intended users. This attack is launched either by deliberately exploiting system vulnerabilities of a victim (e.g., a host, a router, or an entire network) or by flooding a victim with large volume of useless network traffic. Since 1990s, DoS attacks have emerged as a type of the most severe network intrusive behaviours and have posed serious threats to the infrastructures of computer networks and various network-based services.

This thesis aims to provide an intelligent and effective solution for DoS attack detection. Unlike the related works based on machine learning and statistical analysis, this thesis suggests to treat network traffic records as images and to redefine the DoS attack detection problem as a computer vision task.

To achieve the aforementioned objectives, this thesis first conducts a detailed literature review on the state of the art in DoS attack detection. Then, it analyses and chooses the most appropriate mechanisms for DoS attack detection. Afterwards, it designs a general system framework for DoS attack detection with respect to the chosen mechanisms. Furthermore, two Multivariate Correlation Analysis (MCA) approaches are proposed based on two techniques, namely Euclidean distance and triangle area.

These two proposed MCA approaches provide accurate description for network traffic records and facilitate conversion of network traffic into the respective images.

In addition, this thesis proposes a DoS attack detection system, in which the images of network traffic are served as the observed objects and the task of DoS attack detection is reformulated as a computer vision problem, namely image retrieval. This proposed DoS attack detection system applies a widely used dissimilarity measure, namely the Earth Mover's Distance (EMD), to object classification. The EMD takes cross-bin matching into account and provides a more accurate evaluation on the dissimilarity between distributions than some other well-known dissimilarity measures, such as Minkowski-form distance L_p and X^2 statistics. The merits of the EMD facilitate the capability of our proposed system with effective detection.

Last but not least, our intelligent and effective solutions, including the two proposed MCA approaches and the EMD-based DoS attack detection system, are evaluated using the KDD Cup 99 dataset. The evaluation results illustrate that our proposed MCA approaches provide accurate characterisation for network traffic, and the proposed detection system can detect unknown DoS attacks and outperforms two state-of-the-art approaches.

Papers from the Thesis

Papers Appearing in LNCS Series

[1] Zhiyuan Tan, A. Jamdagni, X. He, P. Nanda, R.Liu, Multivariate Correlation Analysis Technique Based on Euclidean Distance Map for Network Traffic Characterization, Information and Communications Security, LNCS, Vol.

7043/2011, pp.388-398. Springer Berlin Heidelberg New York. ISBN: 978-3-642-25242-6.

[2] Zhiyuan Tan, A. Jamdagni, X. He, P. Nanda, R.Liu, Denial-of-Service Attack Detection Based on Multivariate Correlation Analysis. Neural Information Processing, LNCS, Part 3, Vol. 7064/2011, pp.756-765. Springer Berlin Heidelberg New York. ISBN: 978-3-642-24964-8.

[3] Zhiyuan Tan, A. Jamdagni, X. He, P. Nanda, R.Liu, W. Jia, W. Yeh, A Two-tier System for Web Attack Detection Using Linear Discriminant Method, Information and Communications Security, LNCS, Vol. 6476/2010, pp.459-471. Springer Berlin Heidelberg New York. ISBN: 978-3-642-17649-4.

Refereed Journal Articles

[4] Zhiyuan Tan, A. Jamdagni, X. He, P. Nanda, R.Liu, Detection of Denial-of-Service Attacks Based on Computer Vision Techniques, IEEE/ACM Transactions on Networking (IEEE/ACM ToN), Submitted for review on 25th May 2013.

[5] Zhiyuan Tan, A. Jamdagni, X. He, P. Nanda, R.Liu, A System for Denial-of-Service Attack Detection Based on Multivariate Correlation Analysis, IEEE Transactions on Parallel and Distributed Systems (IEEE TPDS), Available online, 03/05/2013. DOI: 10.1109/TPDS.2013.146.

[6] A. Jamdagni, Zhiyuan Tan, P. Nanda, X. He, R. Liu, RePIDS: A Multi Tier Real-Time Payload-Based Intrusion Detection System, Computer Networks, 57(3) 2013, pp. 811-824. ISSN: 1389-1286. DOI: 10.1016/j.comnet.2012.10.002.

[7] A. Jamdagni, Zhiyuan Tan, P. Nanda, X. He, R. Liu, Mahalanobis Distance Map Approach for Anomaly Detection of Web-based Attacks, Journal of Network Forensics, Volume 2 Issue 2, 2010, pp.25-39.

Refereed Conference Papers

[8] Zhiyuan Tan, A. Jamdagni, X. He, P. Nanda, R.Liu, Evaluation on Multivariate Correlation Analysis Based Denial-of-Service Attack Detection System, 1st International Conference on Security of Internet of Things (SecurIT 2012), Kerala, India, 17-19 August, 2012.

[9] Zhiyuan Tan, A. Jamdagni, X. He, P. Nanda, R.Liu, Triangle-Area-Based Multivariate Correlation Analysis for Effective Denial-of-Service Attack Detection, 11th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom-2012), Liverpool, UK, 25-27 June 2012.

[10] Zhiyuan Tan, A. Jamdagni, X. He, P. Nanda, Network Intrusion Detection Based on LDA for Payload Feature Selection, IEEE Globecom 2010 Workshop on Web and Pervasive Security (WPS 2010), Miami, USA, December 6 - 10, 2010, pp.1590-1594. IEEE Communication Society.

[11] A. Jamdagni, Zhiyuan Tan, P. Nanda, X. He, R. Liu, Mahalanobis Distance Map Approach for Anomaly Detection of Web-based Attacks, The 8th Australian Information Security Management Conference, Perth, Australia, November 30 - December 2, 2010, pp.8-17.

[12] A. Jamdagni, Zhiyuan Tan, R. Liu; P. Nanda, X. He, Pattern Recognition Approach for Anomaly Detection of Web-based Attacks, The proceedings of

the seventh annual CSIRO ICT Centre Science and Engineering Conference, CSIRO, Australia, November, 2010.

[13] A. Jamdagni, Zhiyuan Tan, P. Nanda, X. He, R. Liu, Intrusion Detection Using GSAD Model for HTTP Traffic on Web Services, 6th International Wireless Communications and Mobile Computing Conference (IWCMC 2010), Caen, France, June 28 July 2, 2010, pp. 1193-1197. ACM.

[14] A. Jamdagni, Zhiyuan Tan, P. Nanda, X. He, R. Liu, Intrusion Detection Using Geometrical Structures, 4th International Conference on Frontier of Computer Science and Technology (FCST 2009), Shanghai, China, December 17-19, 2009, pp. 327 - 333. IEEE Computer Society.

[15] A. Jamdagni, Zhiyuan Tan, R. Liu; P. Nanda, X. He, A Frame Work for Geometrical Structure Anomaly Detection Model, The proceedings of the sixth annual CSIRO ICT Centre Science and Engineering Conference, CSIRO, Australia, November 11, 2009.

Other Publications

[16] Zhiyuan Tan, Linear Discriminant Analysis Based Feature Selection for Network Intrusion Detection, UTS: FEIT Research Showcase 2010, University of Technology Sydney, Australia, June 2, 2010